



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/069,714

04/26/2002

Michael John Hill

16673-7

4005

7590

05/01/2006

Clifford W Browning

Woodard Emhardt Naughton Moriarty & McNett

Bank One Center Tower

111 Monument Circle Suite 3700

Indianapolis, IN 46204-5137

EXAMINER

ARANI, TAGHI T

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 05/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/069,714	<b>Applicant(s)</b> HILL ET AL.	
	<b>Examiner</b> Taghi T. Arani	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 20 March 2006.  
 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 11-20 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
 6) ☒ Claim(s) 11-20 is/are rejected.  
 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) ☐ All b) ☐ Some \* c) ☐ None of:  
 1. ☐ Certified copies of the priority documents have been received.  
 2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

Taghi T. Arani  
 Primary Examiner  
 AUG 21 2006  
 Taghi T. Arani  
 2/20/06

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 11-20 are pending and examined.

**Continued Examination Under 37 CFR 1.114**

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/07/2006 has been entered.

**Response to Amendment**

3. Applicant's amendment filed 03/07/2006 necessitated the new ground(s) of rejection presented in this Office action. Applicant's arguments with respect to claims 11-20 have been fully considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11 recites the limitation "the immediately preceding encryption/decryption" in line

5. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claim 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, US Patent 5, 768,390 to Coppersmith et al. (hereinafter "Coppersmith") and further in view of US patent 6,330,675 to Wiser et al. (hereinafter "Wiser").

**As per claim 11**, Coppersmith discloses method of encryption and decryption (Abstract) carried out by a plurality of encryption/decryption modules arranged in series (col. 3, lines 29-33 and Fig. 1 and 2), wherein each encryption/decryption module, different from the its preceding module, (col. 5, lines 34-49, and col. 1, lines 41-46).

Coppersmith does not disclose that each module begins encryption/decryption operations before the immediately preceding encryption/decryption module has terminated its encryption/decryption operations.

However, in an analogous art, Wiser discloses a device which securely decrypts and writes an encrypted digital file to a local recordable (Abstract), wherein decryption engine incrementally decrypts the encrypted digital file and an encryption engine then re-encrypts the decrypted portions to form an intermediary file (Wiser, col. 2, lines 20-41). Wiser further teaches a second decryption engine which incrementally decrypts the intermediate file (i.e. the second decryption module (encryption/decryption module)) decrypts incrementally (i.e. begins

Art Unit: 2131

decryption before the first decryption/encryption module has terminated encryption/decryption operations )).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Wiser in the method/system of Coppersmith to have encryption/decryption module of Coppersmith begin encryption/decryption operations before the immediate preceding encryption/decryption module has terminated its encryption/decryption operations, as taught by Wiser's incremental encryption/decryption operations, with a motivation to have substantially less than all of the digital data in decrypted form at any instant , thus significantly reducing the risk of unauthorized copying of the digital data ( Wiser, col. 2, lines 32-41).

**As per claim 12**, Coppersmith as modified discloses method according to Claim 11, wherein a decryption module, different from the immediately preceding module, begins decryption operations as soon as said module receives a part of the results of decryption operations from the immediately preceding decryption module (Wiser, col. 2, lines 29-30, i.e. the second decryption engine incrementally decrypts the intermediate file).

The examiner provides the same rationale as in claim 11 above to combine the teachings of Wiser with Coppersmith.

**As per claim 13**, Coppersmith as modified discloses method according to Claim 11, wherein an encryption module, different from the immediately preceding module, begins encryption operations as soon as said module receives a part of the results of encryption operations from the immediately preceding encryption module (Wiser, col. 2, lines 26-28, the

Art Unit: 2131

encryption engine re-encrypts (incrementally) the decrypted portions to form an intermediate file)).

The examiner provides the same rationale as in claim 11 above to combine the teachings of Wiser with Coppersmith.

**As per claim 14**, Coppersmith discloses method according to Claim 11, carried out by three modules wherein the central module operates with a secret symmetric key (A1, S, A2), (col. 6, lines 59-64 and item 710 of Fig. 7/ three decipherment steps using K1-k3) the central module (S) being of the type with secret symmetric key (k). (col. 6, lines 64-67/DES is a symmetric key encryption which uses the same keys for encryption/decryption).

5. Claims 15-19 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Coppersmith and Wiser in view of prior art of record, Menezes, Van Orschot, Vanstone. Hand Book of Applied Cryptography, 1967, CRC Press, 5<sup>th</sup> Edition 283-291(hereinafter "Menezes").

**As per claim 15**, the combination of Coppersmith and Wiser does not disclose but Menezes discloses method according to claim 14, wherein the first module and the last module in respect of encryption and in reversed order the last module and the first module in respect of decryption operate with an algorithm using asymmetric keys including a private key and a public key (Menezes page 286,8.4, where Menezes discloses using RSA for protecting messages sent over insecure channel using public key to encrypt the message and private key to decrypt the message).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the combination of Coppersmith-Wiser system with the teaching of Menezes to use RSA algorithm in the encryption modules of Coppersmith-Wiser to substitute

Art Unit: 2131

for symmetric encryption modules to overcome the problem of exchanging the decryption keys securely while maintaining the same level of data confidentiality. Furthermore, using symmetric and asymmetric encryption on the same cipher makes it harder for attackers to obtain the private key.

**As per claims 16 and 19**, Menezes teaches using RSA as described in claim 15 where the private key is used for encryption and the public key is used for decryption (page 286, 8.1 and 8.3).

**As per claim 17**, Coppersmith as modified discloses method according to claim 16, wherein the first module and the last module use the same set of private and public keys (col. 4, lines 60 through col. 5, line 7/first encryption is preformed using K1 and the last encryption is performed using the same K1 as well).

**As per claim 18**, Coppersmith as modified discloses method according to Claim 16, wherein the first module and the last module use a different set of private and public keys (col. 6, line 59 through col. 7, line 7/the first module uses K1 and the last module uses K3 rather than K1).

6. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith and Wisner as applied to claim 11 above, and further in view of prior art of record, Golstein et al. US Patent 6,128,735 (prior art of record).

**As per claim 20**, the combination of Coppersmith and Wisner does not disclose but Goldstein discloses method according to Claim 11, carried out by three encryption/decryption modules, wherein all three modules operate with asymmetric keys (Golstein discloses a method

Art Unit: 2131

for transferring data having different sensitivity level (see Abstract) where he teaches the using of encryption using RSA (col. 3, lines 53-66)).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify coppersmith-Wiser method with the teaching of Goldstein to implement all the modules in the system to support asymmetric key encryption because using asymmetric key would eliminate the risk of the shared key being compromised during exchange by enabling the system to communicate securely with other systems by using their public keys. Additionally using asymmetric and symmetric keys in the system enables the system to provide backward capability with system that just provide one method for encryption decryption.

### **Conclusion**

7. Prior arts made of record, not relied upon:

US 5,365,589 to Gutowitz is directed to encryption/decryption and authentication using dynamic systems.

US 5,548,648 to York-Smith discloses encryption method and system which provides a simple encryption method and system for encrypting data into plurality of control and encrypted data blocks.

US 5,742,686 to Finley discloses device and method for dynamic encryption.

US 5,933,501 to Leppek discloses virtual encryption scheme combining different encryption operations into compound mechanism.

Us 6,240,183 to Merchant teaches a data encryption/decryption apparatus which includes plurality of encryption/decryption algorithms.




Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Taghi T. Arani, Ph.D.  
Primary Examiner  
Art Unit 2131  
4/20/06